<u>CLAIMS</u>

We claim:

1.   A method for providing a client with access to a primary system through an intermediate system, said method comprising the steps of:

(a)   creating a log-in record, wherein said log-in record includes an encrypted version of a primary system client identifier;

(b)   said intermediate system receiving log-in data for said client;

(c)   authenticating access of said client to said intermediate system, based on data from said log-in data and data from said log-in record; and

(d)   sending authentication data to said primary system, wherein said authentication data includes data from said primary system client identifier.

2.   The method of claim 1, wherein said step (a) includes the step of:

(1)   encrypting said primary system client identifier.

3.   The method of claim 1, wherein said step (c) includes the steps of:

(1)   identifying said log-in record as corresponding to said log-in data; and

(2)   decrypting said encrypted version of said primary system client identifier in said log-in record to obtain data for said authentication data.

4.   The method of claim 3, wherein said step (c) further includes the step of:

(3)   determining whether said decryption performed in said step (c)(2) is successful.

5.   The method of claim 3, wherein said log-in data includes an intermediate system client identifier and a primary system identifier, wherein said step (c)(1) includes the step of:

(i)   identifying said log-in record as containing a first value corresponding to said intermediate system client identifier and a second value corresponding to said primary system identifier.

6.   The method of claim 3, wherein said step (c)(2) includes the steps of:

(i)   generating a key for decrypting said encrypted version of said primary system client identifier, wherein said step (c)(2)(i) employs an intermediate system client password from said log-in data; and

(ii)   employing said key to decrypt said encrypted version of said primary system client identifier.

7.   The method of claim 6, wherein said step (c)(2)(i) includes the step of:

hashing a combination of said intermediate system client password and at least one value stored in said intermediate system.

8.   The method of claim 1, wherein said encrypted version of said primary system client identifier is expressed as E((tt|CID|CPW), H(IKEY|ICP)), wherein:

E((tt|CID|CPW), H(IKEY|ICP)) is an encrypted value with (tt|CID|CPW) being data encrypted using encryption function E and H(IKEY|ICP) being a key for encryption function E,

(CID|CPW) is said primary system client identifier,

tt is a redundant telltale character string,

H(IKEY|ICP) is a hashed value resulting from hashing data value (IKEY|ICP) with hash function H,

IKEY is an encryption key component stored on said intermediate system,

ICP is as an encryption key component in said log-in data,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

9.   The method of claim 1, wherein said encrypted version of said primary system client identifier is expressed as E((tt|F((CID|CPW), K)), H(IKEY|ICP)), wherein:

E((tt|F((CID|CPW), K)), H(IKEY|ICP)) is an encrypted value with (tt|F((CID|CPW), K)) being data encrypt using encryption function E and H(IKEY|ICP) being a key for encryption function E,

F((CID|CPW),K) is said primary system client identifier, with F((CID|CPW),K) being an encrypted value with (CID|CPW) being data encrypt using encryption function F and K being a key for encryption function F, wherein encryption key K and a corresponding decryption key for encryption function F are known to said primary system and not known to said intermediate system,

tt is a redundant telltale character string,

H(IKEY|ICP) is a hashed value resulting from hashing data value (IKEY|ICP) with hash function H,

IKEY is an encryption key component stored on said intermediate system,

ICP is as an encryption key component in said log-in data,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

10.   The method of claim 1, wherein said encrypted version of said primary system client identifier is expressed as E(F((tt|CID|CPW), K), H(IKEY|ICP)), wherein:

E(F((tt|CID|CPW), K), H(IKEY|ICP)) is an encrypted value with (F(tt|CID|CPW), K) being data encrypted using encryption function E and H(IKEY|ICP) being a key for encryption function E,

F((tt|CID|CPW),K) is said primary system client identifier, with F((tt|CID|CPW),K) being an encrypted value with (tt|CID|CPW) being data encrypted using encryption function F and K being a key for encryption function F, wherein encryption key K and a corresponding decryption key for encryption function F are known to said primary system and not known to said intermediate system,

tt is a redundant telltale character string known to said primary system and not known to said intermediate system,

H(IKEY|ICP) is a hashed value resulting from hashing data value (IKEY|ICP) with hash function H,

IKEY is an encryption key component stored on said intermediate system,

ICP is as an encryption key component in said log-in data,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

11.   The method of claim 1, further including the step of:

(e)   said primary system authenticating access of said client to said primary system, based on said authentication data sent to said primary system in said step (e).

12.   The method of claim 11, wherein said step (e) includes the step of:

(1)   said primary system determining whether at least one value from said authentication data corresponds to said client.

13. The method of claim 12, wherein said authentication data includes a client identifier and a client password, wherein said step (c)(1) includes the step of:

(i) verifying said client identifier and said client password correspond to said client.

14. The method of claim 11, wherein said step (e) includes the steps of:

(1) decrypting said authentication data to obtain a set of data; and

(2) determining whether at least one value from said set of data corresponds to said client.

15. The method of claim 14, wherein said set of data includes a client identifier and a client password, wherein said step (e)(2) includes the step of:

(i) verifying said client identifier and said client password correspond to said client.

16. The method of claim 14, wherein said authentication data is said primary system client identifier.

17. The method of claim 16, wherein said primary system client identifier is expressed as F((CID|CPW),K), wherein:

F((CID|CPW),K) is an encrypted value with (CID|CPW) being data encrypt using encryption function F and K being a key for encryption function F, wherein encryption key K and a corresponding decryption key for encryption function F are known to said primary system and not known to said intermediate system,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

18. The method of claim 16, wherein said primary system client identifier is expressed as F((tt|CID|CPW),K), wherein:

F((tt|CID|CPW),K) is an encrypted value with (tt|CID|CPW) being data encrypted using encryption function F and K being a key for encryption function F, wherein encryption key K and a corresponding decryption key for encryption function F are known to said primary system and not known to said intermediate system,

tt is a redundant telltale character string known to said primary system and not known to said intermediate system,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

19. A processor readable storage medium having processor readable code embodied on said processor readable storage medium, said processor readable code for programming a processor to perform a method for providing a client with access to a primary system through an intermediate system, said method comprising the steps of:

(a)   creating a log-in record, wherein said log-in record includes an encrypted version of a primary system client identifier;

(b)   said intermediate system receiving log-in data for said client;

(c)   authenticating access of said client to said intermediate system, based on data from said log-in data and data from said log-in record; and

(d)   sending authentication data to said primary system, wherein said authentication data includes data from said primary system client identifier.

20. The processor readable storage medium of claim 19, wherein said step (a) includes the step of:

(1)   encrypting said primary system client identifier.

21.   The processor readable storage medium of claim 19, wherein said step (c) includes the steps of:

(1)   identifying said log-in record as corresponding to said log-in data; and

(2)   decrypting said encrypted version of said primary system client identifier in said log-in record to obtain data for said authentication data.

22.   The processor readable storage medium of claim 21, wherein said log-in data includes an intermediate system client identifier and a primary system identifier, wherein said step (c)(1) includes the step of:

(i)   identifying said log-in record as containing a first value corresponding to said intermediate system client identifier and a second value corresponding to said primary system identifier.

23.   The processor readable storage medium of claim 21, wherein said step (c)(2) includes the steps of:

(i)   generating a key for decrypting said encrypted version of said primary system client identifier, wherein said step (c)(2)(i) employs an intermediate system client password from said log-in data; and

(ii)   employing said key to decrypt said encrypted version of said primary system client identifier.

24.   The processor readable storage medium of claim 23, wherein said step (c)(2)(i) includes the step of:

hashing a combination of said intermediate system client password and at least one value stored in said intermediate system.

25.   The processor readable storage medium of claim 19, wherein said encrypted version of said primary system client identifier is expressed as $E((tt|CID|CPW), H(IKEY|ICP))$, wherein:

E((tt|CID|CPW), H(IKEY|ICP)) is an encrypted value with (tt|CID|CPW) being data encrypted using encryption function E and H(IKEY|ICP) being a key for encryption function E,

(CID|CPW) is said primary system client identifier,

tt is a redundant telltale character string,

H(IKEY|ICP) is a hashed value resulting from hashing data value (IKEY|ICP) with hash function H,

IKEY is an encryption key component stored on said intermediate system,

ICP is as an encryption key component in said log-in data,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

26. The processor readable storage medium of claim 19, wherein said encrypted version of said primary system client identifier is expressed as E((tt|F((CID|CPW), K)), H(IKEY|ICP)), wherein:

E((tt|F((CID|CPW), K)), H(IKEY|ICP)) is an encrypted value with (tt|F((CID|CPW), K)) being data encrypt using encryption function E and H(IKEY|ICP) being a key for encryption function E,

F((CID|CPW),K) is said primary system client identifier, with F((CID|CPW),K) being an encrypted value with (CID|CPW) being data encrypt using encryption function F and K being a key for encryption function F, wherein encryption key K and a corresponding decryption key for encryption function F are known to said primary system and not known to said intermediate system,

tt is a redundant telltale character string,

H(IKEY|ICP) is a hashed value resulting from hashing data value (IKEY|ICP) with hash function H,

IKEY is an encryption key component stored on said intermediate system,

ICP is as an encryption key component in said log-in data,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

27. The processor readable storage medium of claim 19, wherein said encrypted version of said primary system client identifier is expressed as E(F((tt|CID|CPW), K), H(IKEY|ICP)), wherein:

E(F((tt|CID|CPW), K), H(IKEY|ICP)) is an encrypted value with (F(tt|CID|CPW), K) being data encrypted using encryption function E and H(IKEY|ICP) being a key for encryption function E,

F((tt|CID|CPW),K) is said primary system client identifier, with F((tt|CID|CPW),K) being an encrypted value with (tt|CID|CPW) being data encrypted using encryption function F and K being a key for encryption function F, wherein encryption key K and a corresponding decryption key for encryption function F are known to said primary system and not known to said intermediate system,

tt is a redundant telltale character string known to said primary system and not known to said intermediate system,

H(IKEY|ICP) is a hashed value resulting from hashing data value (IKEY|ICP) with hash function H,

IKEY is an encryption key component stored on said intermediate system,

ICP is as an encryption key component in said log-in data,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

28. The processor readable storage medium of claim 19, further including the step of:

(e) said primary system authenticating access of said client to said primary system, based on said authentication data sent to said primary system in said step (e).

29.   The processor readable storage medium of claim 28, wherein said step (e) includes the step of:

(1)   said primary system determining whether at least one value from said authentication data corresponds to said client.

30.   The processor readable storage medium of claim 29, wherein said authentication data includes a client identifier and a client password, wherein said step (c)(1) includes the step of:

(i)   verifying said client identifier and said client password correspond to said client.

31.   The processor readable storage medium of claim 28, wherein said step (e) includes the steps of:

(1)   decrypting said authentication data to obtain a set of data; and

(2)   determining whether at least one value from said set of data corresponds to said client.

32.   The processor readable storage medium of claim 31, wherein said set of data includes a client identifier and a client password, wherein said step (e)(2) includes the step of:

(i)   verifying said client identifier and said client password correspond to said client.

33.   The processor readable storage medium of claim 31, wherein said authentication data is said primary system client identifier.

34.   The processor readable storage medium of claim 33, wherein said primary system client identifier is expressed as F((CID|CPW),K), wherein:

F((CID|CPW),K) is an encrypted value with (CID|CPW) being data encrypt using encryption function F and K being a key for encryption function

F, wherein encryption key K and a corresponding decryption key for encryption function F are known to said primary system and not known to said intermediate system,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

35. The processor readable storage medium of claim 33, wherein said primary system client identifier is expressed as F((tt|CID|CPW),K), wherein:

F((tt|CID|CPW),K) is an encrypted value with (tt|CID|CPW) being data encrypted using encryption function F and K being a key for encryption function F, wherein encryption key K and a corresponding decryption key for encryption function F are known to said primary system and not known to said intermediate system,

tt is a redundant telltale character string known to said primary system and not known to said intermediate system,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

36. An apparatus providing a client with access to a primary system through an intermediate system, said apparatus comprising:

a processor; and

a processor readable storage medium, in communication with said processor, said processor readable storage medium storing code for programming said processor to perform a method including the steps of:

(a)   creating a log-in record, wherein said log-in record includes an encrypted version of a primary system client identifier;

(b)   said intermediate system receiving log-in data for said client;

(c)   authenticating access of said client to said intermediate system, based on data from said log-in data and data from said log-in record; and

(d)   sending authentication data to said primary system, wherein said authentication data includes data from said primary system client identifier.

37.   The apparatus of claim 36, wherein said step (a) includes the step of:

(1)   encrypting said primary system client identifier.

38.   The apparatus of claim 36, wherein said step (c) includes the steps of:

(1)   identifying said log-in record as corresponding to said log-in data; and

(2)   decrypting said encrypted version of said primary system client identifier in said log-in record to obtain data for said authentication data.

39.   The apparatus of claim 38, wherein said step (c)(2) includes the steps of:

(i)   generating a key for decrypting said encrypted version of said primary system client identifier, wherein said step (c)(2)(i) employs an intermediate system client password from said log-in data; and

(ii)   employing said key to decrypt said encrypted version of said primary system client identifier.

40.   The apparatus of claim 39, wherein said step (c)(2)(i) includes the step of:

hashing a combination of said intermediate system client password and at least one value stored in said intermediate system.

41.   The apparatus of claim 36, wherein said encrypted version of said primary system client identifier is expressed as E((tt|CID|CPW), H(IKEY|ICP)), wherein:

E((tt|CID|CPW), H(IKEY|ICP)) is an encrypted value with (tt|CID|CPW) being data encrypted using encryption function E and H(IKEY|ICP) being a key for encryption function E,

(CID|CPW) is said primary system client identifier,

tt is a redundant telltale character string,

H(IKEY|ICP) is a hashed value resulting from hashing data value (IKEY|ICP) with hash function H,

IKEY is an encryption key component stored on said intermediate system,

ICP is as an encryption key component in said log-in data,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

42.   The apparatus of claim 36, wherein said encrypted version of said primary system client identifier is expressed as E((tt|F((CID|CPW), K)), H(IKEY|ICP)), wherein:

E((tt|F((CID|CPW), K)), H(IKEY|ICP)) is an encrypted value with (tt|F((CID|CPW), K)) being data encrypt using encryption function E and H(IKEY|ICP) being a key for encryption function E,

F((CID|CPW),K) is said primary system client identifier, with F((CID|CPW),K) being an encrypted value with (CID|CPW) being data encrypt using encryption function F and K being a key for encryption function F, wherein encryption key K and a corresponding decryption key for encryption function F are known to said primary system and not known to said intermediate system,

tt is a redundant telltale character string,

H(IKEY|ICP) is a hashed value resulting from hashing data value (IKEY|ICP) with hash function H,

IKEY is an encryption key component stored on said intermediate system,

ICP is as an encryption key component in said log-in data,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.

43.   The apparatus of claim 36, wherein said encrypted version of said primary system client identifier is expressed as E(F((tt|CID|CPW), K), H(IKEY|ICP)), wherein:

E(F((tt|CID|CPW), K), H(IKEY|ICP)) is an encrypted value with (F(tt|CID|CPW), K) being data encrypted using encryption function E and H(IKEY|ICP) being a key for encryption function E,

F((tt|CID|CPW),K) is said primary system client identifier, with F((tt|CID|CPW),K) being an encrypted value with (tt|CID|CPW) being data encrypted using encryption function F and K being a key for encryption function F, wherein encryption key K and a corresponding decryption key for encryption function F are known to said primary system and not known to said intermediate system,

tt is a redundant telltale character string known to said primary system and not known to said intermediate system,

H(IKEY|ICP) is a hashed value resulting from hashing data value (IKEY|ICP) with hash function H,

IKEY is an encryption key component stored on said intermediate system,

ICP is as an encryption key component in said log-in data,

CID is a client identifier corresponding to said client, and

CPW is a client password corresponding to said client.